



**Communications and Information**

**UNIT COMPLIANCE INSPECTION  
CHECKLIST - INFORMATION ASSURANCE**

**NOTICE:** This publication is available digitally on the AFDPO WWW site at:  
<http://www.e-publishing.af.mil>.

OPR: HQ USAFE/A6XF  
(CMSgt Samuel Mitchell)

Certified by: HQ USAFE/A6X  
(Col Mona Lisa D. Tucker)  
Pages: 7  
Distribution: F

This publication implements Air Force Policy Directive (AFPD) 33-1, *Command, Control, Communications, and Computer (C4) Systems*. The Inspection Checklist is developed to support AFI 90-201, *Inspector General Activities*, and the USAFE Supplement 1, inspection programs. This checklist is intended for inspection use. The checklist identifies compliance items that support policy established by AFI 33-115, Vol 1, *Network Operations (NETOPS)*, AFI 33-202, Vol 1, *Computer and Network Security*, AFI 33-203, Vol 1, *Emission Security*, and AFI 33-201 Vol 2, *Communications Security (COMSEC) User Requirements*. It applies to all United States Air Forces in Europe (USAFE) Network Operations and Security Center (NOSC), Network Control Center (NCC), and Wing Information Assurance (IA) offices. It does not apply to Air National Guard (ANG) or Air Force Reserve Command (AFRC) units. Send comments and suggested improvements to this publication on AF IMT 847, **Recommendation for Change of Publication**, to Force Management and Readiness Branch (HQ USAFE/A6XF), Unit 3050 Box 125, APO AE 09094. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with AFMAN 37-123, *Management of Records* and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located at: <https://afirms.amc.af.mil>.

**1. General.** The items listed do not constitute the order or limit the scope of the inspection or assessment. As a minimum, units should use this inspection checklist in conjunction with the Unit Self-Assessment. The objective is to identify deficiencies that preclude attainment of required capabilities. Higher headquarters may use this checklist in whole or in part during visits or exercises.

**1.1. Core Compliance Guide Items (CCGI) and Compliance Guide Items (CGI).** Items identified by functional managers to prioritize command requirements and to allow the Inspector General (HQ USAFE/IG) inspectors to assess criticality of deficiencies.

**1.1.1. CCGI.** Items identified by HQ USAFE directorates and functional managers as key result areas for successful mission accomplishment including, but not limited to, items where non-compliance could result in serious injury, loss of life, excessive cost, litigation or affect system reliability. These requirements may be mandated by law, Executive Order, Department of Defense (DoD)

directive, safety or Air Force and USAFE strategic plans. CCGIs are referred to as significant guide items requiring direct IG evaluation. Identify CCGIs by using uppercase and bold letters.

1.1.2. **CGI.** CGI are areas that require special vigilance and are important to the overall performance of the unit. Noncompliance could result in some negative impact on mission performance but is not likely to result in injury, unnecessary cost, or litigation. Identify CGIs by using standard sentence case.

**2. Applicability.** All items on this guide are assigned an applicability code designating the wing/unit/installation to which the item applies. Reference for the applicability code is AFI 90-201\_USAFE SUP1 , Table A11.2., Inspection Applicability Table.

**2.1. IMTs Adopted:** AF IMT 847, **Recommendation for Change of Publication**, AF IMT 4160, **Information Assurance Assessment and Assistance Program (IAPP) Criteria**.

**Table 1. Inspection Items for Information Assurance.**

<b>Item No.</b>	<b>Item</b>	<b>Reference</b>	<b>Applica-bility Code</b>	<b>Yes/ No</b>	
<b>1.</b>	<b>COMPUTER SECURITY (COMPUSEC)</b>				
1.1.	Does Wing IA ensure Client Support Administrators (CSA) promote user awareness concerning unauthorized or illegal use of computer hardware and software?	AFI 33-115V1, Para 4.8.15.	3,5,7,8		
1.2.	Do all network users have a favorable background investigation, are trained, and licensed?	AFI 33-115V2 Para 5.1.,5.3., & AFI 33-202V1, Para 3.9.1.	3,5,7,8		
1.3.	Does Wing IA semiannually verify with the NCC that only accredited systems and applications (classified and unclassified) are connected to or use the base network?	AFI 33-202V1, Para 2.16.2.3.	3,5,7,8		
1.4.	Does Wing IA respond to suspected incidents of contaminated systems and ensure remanence security is implemented?	AFI 33-202V1, Para 2.16.2.8.	3,5,7,8		
1.5.	Does Wing IA ensure a role-based access scheme that accounts for all privileged access and implements the principles of least privilege and separation of functions is utilized?	AFI 33-202V1, Para 2.16.2.12.	3,5,7,8		
1.6.	Does Wing IA ensure all software is included in the System Security Authorization Accreditation (SSAA) for the system?	AFI 33-202V1, Para 3.3.1.	3,5,7,8		
1.7.	Has Wing IA established procedures to rapidly obtain, distribute, and install changes to antivirus software on all information systems (including network servers)?	AFI 33-202V1, Para 3.8.1.4.	3,5,7,8		
1.8.	Does Wing IA verify each user's need for access to information system resources and information?	AFI 33-202V1, Para 4.1.1.1.	3,5,7,8		
1.9.	Does Wing IA implement auditing for information systems?	AFI 33-202V1, Para 4.2.1.8.	3,5,7,8		

Item No.	Item	Reference	Applica-bility Code	Yes/No
1.10.	Are non-U.S. citizens categorized as Information Technology Position Access Level 1 (IT-I) and Access Level 2 (IT-II) (formerly known as Automation Information system Position Access Level I (AIS-I) and Access Level 2 (AIS-II) positions under the immediate supervision of a U.S. citizen?	AFI 33-202V1, Para 5.2.2.	3,5,7,8	
1.11.	Does Wing IA ensure IA awareness is available to all information system users, including all tenant units and all geographically separated units (GSU)?	AFI 33-204, Para 14.2.	3	
1.12.	Does Wing IA perform annual IA self-assessments on behalf of the wing commander, using the required AF IMT 4160, <b>Information Assurance Assessment and Assistance Program (IAPP) Criteria?</b>	AFI 33-230, Para 2.5.1.	3	
2.	<b>EMANATION SECURITY (EMSEC)</b>			
2.1.	Has the Wing IA office properly trained the EMSEC Manager?	AFI 33-203, Para 2.9.2.	3	
2.2.	Are units contacting the Wing IA office whenever they intend to process classified information (i.e., new facility, new processing environment)?	AFI 33-203, Para 3.1.	3,5,7,8	
2.3.	Has the Wing IA office submitted completed EMSEC countermeasures for Air Force Certified Technical TEMPEST Authority (CTTA) validation?	AFI 33-203, Para 3.3.	3	
2.4.	Has the Wing IA office properly performed and documented EMSEC assessments on all systems that process classified national security information?	AFI 33-203, Para 1.1.2.	3	
3.	<b>COMMUNICATIONS SECURITY (COMSEC)</b>			
3.1.	Has the installation commander or supporting commander appointed a COMSEC Manager and alternate?	AFKAG-1N, Para 2.1.5.2.	3,5,7,8	

Item No.	Item	Reference	Applicability Code	Yes/No
3.2.	Has the unit commander appointed, by letter, a primary COMSEC Responsible Officer (CRO) and at least one alternate to receive COMSEC material from the account?	AFI 33-201 V2, Para 4.	3,5,7,8	
4.	<b>Network Control Center (NCC)</b>			
4.1.	Does NOSC/NCC implement Time Compliance Network Orders (TCNO), execute changes, and/or perform "touch labor" as directed by major command (MAJCOM) NOSC?	AFI 33-115V1, Para 4.6.4.1.	1,3,5,7,8	
4.2.	Does NOSC/NCC perform regular day-to-day system backup and recovery operations on NCC managed servers?	AFI 33-115V1, Para 4.6.5.12.	1,3,5,7,8	
4.3.	Does NOSC/NCC, at a minimum of once a quarter, test recovery procedures to ensure procedures are accurate and operational?	AFI 33-115V1, Para 4.6.5.12.	1,3,5,7,8	
4.4.	Does NOSC/NCC develop local restoral and contingency operations plans from existing operations/war plans and validate restoral plans by testing them on at least a biannual basis?	AFI 33-115V1, Para 4.6.5.13.	1,3,5,7,8	
4.5.	Does NOSC/NCC distribute and install network software releases and updates, and assist customers with software installation and customization?	AFI 33-115V1, Para 4.6.5.16.8.2.1.	1,3,5,7,8	
4.6.	Does NOSC/NCC perform vulnerability assessments to test and validate security of networks and systems?	AFI 33-115V1, Para 4.6.5.18.1.2.	1,3,5,7,8	
4.7.	Does NOSC/NCC conduct daily traffic analysis, identify and characterize incidents, and generate incident reports with Air Force approved intrusion detection tools?	AFI 33-115V1, Para 4.6.5.18.1.3.	1,3,5,7,8	
4.8.	Does NOSC/NCC ensure all systems and networks meet Air Force and local security requirements and have appropriate Designated Approval Authority (DAA) approval before connecting to the base network infrastructure?	AFI 33-115V1, Para 4.6.5.18.2.	1,3,5,7,8	

Item No.	Item	Reference	Applica-bility Code	Yes/No
4.9.	Does NOSC/NCC equip all servers within the Combat Information Transport System (CITS) Network Operation /Information Assurance (NO/IA) boundary with host-based intrusion detection and network security analysis and scanning tools?	AFI 33-115V1, Para 4.6.5.18.3.2.	1,3,5,7,8	
4.10.	Does NCC ensure Functional System Administrators implement network security policies and procedures as outlined in the base/ MAJCOM network security policy?	AFI 33-115V1, Para 4.7.10.	3,5,7,8	
4.11.	Does the NCC serve as the wing/base office of primary responsibility (OPR) to acknowledge, disseminate, and implement TCNOs and C4 Notice to Airmen (NOTAM) and to track and report compliance with TCNOs?	AFI 33-138, Para 2.8.1.	3,5,7,8	
4.12.	Does the NCC track, compile, assess, and report to their parent NOSC all unauthorized activities and incidents that occur on any network or system under the NCC's purview?	AFI 33-138, Para 2.8.3.4.	3,5,7,8	
4.13.	Does the NOSC/NCC ensure audit trail records from all core network services and infrastructure devices are regularly reviewed for indications of inappropriate or unusual activity?	AFI 33-202, Para 2.16.4.8.	1,3,5,7,8	
4.14.	Does the NOSC/NCC review account usage for systems every 6 months to help identify dormant accounts on the system?	AFMAN 33-223, Para 5.4.	1,3,5,7,8	
4.15.	Does the NOSC/NCC/Functional System Administrator (FSA) utilize password policy enforcer and monthly use of password cracking tools?	AFMAN 33-223, Para 5.7. 5.7.1.1., & 5.7.1.2.	1,3,5,7,8	

STEVEN J. SPANO, Colonel, USAF  
 Director, Communications and Information Directorate

**Attachment 1****GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

AFPD 33-1, *Command, Control, Communications and Computer (C4) Systems*  
AFI 33-115 Volume 1, *Network Operations (NETOPS)*  
AFI 33-115 Volume 2, *Licensing Network Users and Certifying Network Professionals*  
AFI 33-138, *Enterprise Network Operations Notification and Tracking*  
AFI 33-201 Volume 2, *Communications Security (COMSEC) User Requirements*  
AFI 33-202 Volume 1, *Network and Computer Security*  
AFI 33-203 Volume 1, *Emission Security*  
AFI 33-204, *Information Assurance (IA) Awareness Program*  
AFMAN 33-223, *Identification and Authentication*  
AFI 33-230, *Information Assurance Assessment and Assistance Program*  
AFMAN 37-123, *Management of Records*  
AFI 90-201, *Inspector General Activities*, and the USAFE Supplement 1  
AFKAG-IN, *Air Force Communications Security (COMSEC) Operations*

***Abbreviations and Acronyms***

**C4**—Command, Control, Communications and Computer  
**CCGI**—Core Compliance Guide Item  
**CGI**—Compliance Guide Item  
**COMSEC**—Communications Security  
**EMSEC**—Emanation Security  
**IA**—Information Assurance  
**IG**—Inspector General  
**MAJCOM**—Major Command  
**NCC**—Network Control Center  
**NOSC**—Network Operations and Security Center  
**TCNO**—Time Compliance Network Order  
**USAFE**—United States Air Forces in Europe